This Data Processing Addendum (the "DPA") is incorporated into and supplements the terms and conditions of the TimeClock Plus OnDemand License Agreement or the TimeClock Plus Perpetual Terms and Conditions, each available at https://www.timeclockplus.com/..., or other agreement between you ("Client") and TimeClock Plus, LLC ("TCP") governing Client's use of the software products and services provided by TCP to Client from time to time (the "TCP Services") (such agreement between TCP and Client, the "Agreement"). For the avoidance of doubt, all references to the "Agreement" shall include this DPA. TCP and Client may individually be referred to as a "Party", and collectively as the "Parties".

1. **Definitions.**
    a. "Affiliate" means any parent or subsidiary corporation, and any corporation or other business entity controlling, controlled by or under common control with a Party.
    b. "Biometric Data" means any information based on an individual's retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry which is used to identify an individual, regardless of how it is captured, converted, stored or shared.
    c. "Client Data" means all of Client's data processed or stored by or transmitted to TCP in connection with the Agreement, including, without limitation, all Personal Data contained therein.
    d. "Designated User" means the individual Employees who are authorized by Client to use the TCP Services on behalf of the Client, and whose Personal Data may be processed or stored by or transmitted to TCP in connection with the Agreement.
    e. "Employee" means Client's individual employee, worker, consultant, substitute or contractor.
    f. "Global Data Privacy Policy" means TCP's Global Data Privacy Policy located at https://www.timeclockplus.com/..., as updated from time to time.
    g. "Personal Data" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Employee or Designated User.
    h. "Subprocessor" means any third party entity that processes Personal Data on behalf of TCP and to which TCP discloses Personal Data for a business purpose pursuant to a written contract, provided that the contract prohibits such entity from retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services identified in such contract.
2. **Data Processing.**

a. TCP shall provide the TCP Services to Client in accordance with, and Client's use of the TCP Services is subject to, the terms and conditions of the Agreement and the Global Data Privacy Policy.
b. Client hereby grants TCP a worldwide, royalty-free, non-exclusive, limited license to use, host, copy, transmit, display, modify and create derivative works of Client Data for the express purpose of providing the TCP Services. Client acknowledges and agrees that it will determine the means and purposes of processing Client Data, and that TCP acts solely as a service provider that processes Client Data on behalf of and at the direction of Client for the sole purpose of performing the TCP Services under the Agreement. Client is responsible for ensuring that all Designated Users who provide instructions to TCP on Client's behalf are authorized to do so. Client shall have sole responsibility for the accuracy, quality, content, legality and use of Client Data and the means by which any Personal Data is obtained from Designated Users and Employees and transferred to TCP, and Client is solely responsible for any transfer of Personal Data to any third party data controller or data processor (e.g., human resources or payroll application), and TCP shall have no liability in connection therewith. Client agrees to implement data protection-related procedures that will not be less protective than those imposed on TCP by the Agreement and the Global Data Privacy Policy.
c. TCP is expressly prohibited from processing any Client Data for any purpose other than for the specific purpose of performing the TCP Services, unless requested by Client or required by applicable law. TCP is expressly prohibited from selling Personal Data under any circumstances and for any purpose. No other collection, use, disclosure or transfer (except to Subprocessors in accordance with Section 3) of Client Data is permitted without the express prior written instruction of Client. TCP acknowledges and agrees that it understands and will comply with each of the restrictions and obligations set forth in this Section 2.3.

3. **Subprocessors.**
   a. TCP has appointed Subprocessors for the purpose of providing data hosting and security services. Client acknowledges and agrees that Subprocessors may process Client Data in accordance with the terms of the Agreement and the Global Data Privacy Policy. TCP's agreements with its Subprocessors impose data protection-related processing terms on such Subprocessors that are not less protective than the terms imposed on TCP in the Agreement and the Global Data Privacy Policy. The Global Data Privacy Policy contains an overview of the categories of Subprocessors involved in the performance of the

relevant TCP Services. The appointment of a Subprocessor to perform part or all of the TCP Services hereunder shall not relieve TCP of any liability under the Agreement.

4. **Data Security.**
    a. Security Standards.
        i. TCP shall implement reasonable security procedures consistent with industry standards to protect Client Data from unauthorized access, including without limitation (i) industry-standard encryption of data at rest within TCP's data centers; (ii) web application firewalls; (iii) virus detection and anti-virus software; (iv) authentication techniques, such as user names and passwords, or authorization formats, which limit access to particular TCP personnel; and (v) additional security controls consistent with SOC 2 Type II reporting standards.
        ii. The Parties shall implement administrative, technical and physical security procedures consistent with industry standards and applicable data protection laws to protect Client Data from unauthorized access, including by adopting access policies that prevent the internal sharing or inadvertent communication of login credentials.
        iii. Client is responsible for reviewing the information made available by TCP relating to data security and making an independent determination as to whether the TCP Services meet Client's requirements and obligations under applicable data protection laws. Client acknowledges that data security measures taken by TCP are subject to technical progress and development and TCP may update or modify such security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the TCP Services.
    b. Security Breach Notifications. TCP will promptly report to Client any unauthorized access to Client Data within TCP's or its Subprocessors' systems upon discovery and in accordance with applicable data breach notification laws. TCP will use diligent efforts to promptly remedy any breach of security that permitted such unauthorized access. TCP's notification of or response to any security incident under this Section 4.2 shall not be construed as an acknowledgment by TCP of any fault or liability with respect to such security incident.
    c. Data Backup and Retention. TCP shall undertake commercially reasonable efforts to backup Client Data with a restore point objective of twenty-four (24) hours. Client Data shall be backed up and retained

in accordance with TCP's retention policy as set forth in the Global Data Privacy Policy.

5. **Data Privacy.** TCP will process Client Data in accordance with the terms of the Agreement, the Global Data Privacy Policy and all applicable data protection laws. Client must maintain its own data collection, disclosure, retention, and storage policies in compliance with applicable law.
    a. Biometric Data. To the extent that Client collects, captures, stores, or otherwise uses Biometric Data relating to an individual, Client must (i) first inform the individual from whom Biometric Data will be collected, in writing and prior to collecting his or her Biometric Data, that Biometric Data is being collected, stored, and/or used; (ii) indicate, in writing, the specific purpose(s) (which may not be other than employment-related purposes) and length of time for which Biometric Data is being collected, stored, and/or used; and (iii) receive a written release from the individual (or his or her legally authorized representative) authorizing the Client, TCP, and TCP's third-party service providers (who are subject to restrictions no less restrictive than those imposed on TCP herein) to collect, store, and/or use the Biometric Data and authorizing the Client to disclose such Biometric Data to TCP and TCP's third-party service providers.
    b. Requests. Client agrees to adopt a commercially reasonable policy for managing data requests from Designated Users and Employees, which policy shall safeguard the rights of such data subjects and respect the original purpose of such data collection. Client, as the Party who determines the means and purposes for processing Client Data, shall be responsible for receiving, investigating, documenting, and responding to all Designated User and Employee requests for inspection or erasure of Personal Data.
    c. Assistance. If Client receives a request from a Designated User or Employee to exercise such individual's rights under applicable data protection laws, and Client requires TCP's assistance to respond to such request in accordance with applicable data protection laws, TCP shall assist the Client by providing any necessary information and documentation that is under TCP's control. TCP shall be given reasonable time to assist the Client with such requests in accordance with applicable law.
    d. Privacy Policy. Where required by law, Client agrees to adopt a privacy policy in alignment with the Agreement and all applicable laws governing the collection, use, transfer and retention of Personal Data. Client agrees to provide TCP, upon reasonable request, Client's adopted privacy policy.
6. **Access to Third Party Platforms.**

a. Client may require the TCP Services to interoperate with platforms or other online services operated by third parties ("Third-Party Platforms") pursuant to an agreement between TCP and the operators of such Third-Party Platforms, an agreement between Client and the operators of such Third-Party Platforms, or through application programming interfaces ("APIs") or other means of interoperability which are generally made available by such operators.
b. Client hereby grants TCP the limited right to access such Third-Party Platforms with Client's credentials and on behalf of the Client in connection with the performance of the TCP Services. Client acknowledges and agrees that TCP's agreements with the operators of such Third-Party Platforms and the terms governing the use of APIs may be modified, suspended or terminated at any time, and TCP shall have no liability with respect to any such modification, suspension or termination. Client is responsible for ensuring that its use of the TCP Services in connection with any Third-Party Platform, and TCP's access to such Third-Party Platforms on Client's behalf, complies with all agreements and terms applicable to such Third-Party Platform.

7. **Confidentiality.** TCP will not access or use, or disclose to any third party (except to Subprocessors in accordance with Section 3), Client Data, except, in each case, as necessary to maintain or provide the TCP Services, or as necessary to comply with applicable law or a subpoena or inquiry issued by a court of competent jurisdiction or by a judicial or administrative agency or legislative body or committee (a "Governmental Entity"). If TCP is requested to disclose all or any part of any Client Data under a subpoena or inquiry issued by a Governmental Entity, TCP shall (i) immediately notify Client of the existence, terms and circumstances surrounding such request; (ii) consult with Client on the advisability of taking legally available steps to resist or narrow such request and cooperate with Client on any such steps it considers advisable; and (iii) if disclosure of the Client Data is required or deemed advisable, exercise its best efforts to obtain an order, stipulation or other reasonably acceptable assurance that the Client Data or part thereof required to be disclosed shall retain its confidentiality and remain otherwise subject to the Agreement.
8. **Term; Termination.** This DPA shall continue in force until the termination of the Agreement. Upon any termination or expiration of the Agreement, TCP will permanently delete any and all copies of Client Data created, processed and/or stored pursuant to this Agreement, subject to the terms of the Agreement.
9. **Client Representations and Warranties.**
    a. Client represents and warrants that the performance of Client's obligations and use of the TCP Services by Client, its Designated Users

and Employees will not violate any applicable laws, including all applicable domestic and international data protection laws, or cause a breach of duty to any third party, including Employees.

b. Client represents and warrants that all Personal Data included in the Client Data has been collected from all Employees and Designated Users and will be transferred to TCP in accordance with all applicable data protection laws, including, but not limited to, the EU General Data Protection Regulation 2016/679 and the Illinois Biometric Information Privacy Act, to the extent applicable. Client acknowledges and agrees that (i) TCP is a service provider and processes Client Data solely on behalf of and at the direction of Client, and exercises no control whatsoever over the content of the Client Data passing through the TCP Services or that is otherwise transferred by Client to TCP, and (ii) it is the sole responsibility of Client to ensure that the Client Data passing through the TCP Services or that is otherwise transferred by Client to TCP complies with all applicable laws and regulations, whether now in existence or hereafter enacted and in force.

c. In the event of any breach of any of the foregoing representations or warranties in this Section 9, in addition to any other remedies available at law or in equity, TCP will have the right to suspend immediately any TCP Services if deemed reasonably necessary by TCP to prevent any harm to TCP and its business. TCP will provide notice to Client and an opportunity to cure, if practicable, depending on the nature of the breach. Once cured, TCP will promptly restore the TCP Services.

10. **TCP Representations and Warranties.** TCP represents and warrants that the performance of its obligations and delivery of the TCP Services to Client will not violate any applicable laws or regulations of the United States or cause a breach of any agreements between TCP and any third parties.
11. **Mutual Representations and Warranties.** Each Party represents and warrants that it has implemented a comprehensive written information security program that includes appropriate administrative, technical and physical safeguards to: (i) ensure the safety and confidentiality of Personal Data; (ii) protect against unauthorized access to and use of Personal Data; (iii) protect against anticipated threats or hazards to the security or integrity of Personal Data, and (iv) comply with all applicable data protection laws.
12. **Indemnification.** Client hereby acknowledges and agrees that TCP may not be aware of all rights available to Client's Designated Users or Employees under all data protection regimes. To the extent permitted by applicable law, Client shall indemnify, defend and hold harmless TCP, its Affiliates, Subprocessors, officers, managers, directors, employees, agents, advisors and other representatives (the "TCP Indemnitees") from and against any lawsuit, liability, loss, cost or expense (including reasonable attorneys' fees) actually incurred

or suffered by TCP Indemnitees of every kind and nature to the extent caused by or resulting from (i) any breach of a representation or warranty made by Client under this Agreement; or (ii) a third-party claim made against a TCP Indemnitee arising from or related to Client's failure to comply with any applicable domestic or foreign data protection laws or regulations. Client shall have the right to control any defense provided pursuant to this Section 12, provided, however, that Client shall not, without TCP's prior written consent, (A) enter into any settlement or compromise or consent to the entry of any judgment that does not include the delivery by the claimant or plaintiff to the applicable TCP Indemnitee of a written release from all liability in respect of such third-party claim, or (B) enter into any settlement or compromise with respect to any third-party claim that may adversely affect the applicable TCP Indemnitee other than as a result of money damages or other monetary payments that are indemnified hereunder.

13. **Limitation of Liability.** Except for claims arising out of Section 7 (Confidentiality), in no event shall TCP's aggregate liability, if any, including liability arising out of contract, negligence, strict liability in tort or warranty, or otherwise, exceed the sum of amounts paid by Client to TCP during the six (6) months immediately prior to the date of the claim.
14. **Entire Agreement; Conflict.** Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between this DPA and any other agreement between the Parties (including the Agreement, but excluding the Global Data Privacy Policy), the terms of this DPA will control. If there is a conflict between the Global Data Privacy Policy and any other agreement between the Parties (including this DPA and the Agreement), the Global Data Privacy Policy will control.

Agreed by:

Client	
By:	
Name:	
Dated:	

TimeClock Plus, LLC.
By:
Name:
Dated: